STUDY PROJECT

JOINT INTELLIGENCE IN A CHANGING DEFENSE ESTABLISHMENT: THE CASE OF COUNTERINTELLIGENCE

BY

TED R. SNEDIKER
United States Department of the Army Civilian

USAWC CLASS OF 1993

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release. Distribution is unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION U.S. ARMY WAR COLLEGE 6b. OFFICE SYMBOL (*If applicable*)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (*City, State, and ZIP Code*) ROOT HALL, BUILDING 122 CARLISLE, PA 17013-5050	7b. ADDRESS (*City, State, and ZIP Code*)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (*If applicable*)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City, State, and ZIP Code*)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.

11. TITLE (*Include Security Classification*)
JOINT INTELLIGENCE IN A CHANGING DEFENSE ENVIRONMENT: THE CASE OF COUNTERINTELLIGENCE

12. PERSONAL AUTHOR(S)
Ted R. Snediker, Army Civilian

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (*Year, Month, Day*)	15. PAGE COUNT
Individual	FROM _____ TO _____	93 March 22	58

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUB-GROUP	

19. ABSTRACT (*Continue on reverse if necessary and identify by block number*) The reexamination of Defense intelligence roles, functions and organizational structures stimulated by the Goldwater-Nichols Act of 1986 and subsequent changes in the global and fiscal environments includes the counter-intelligence (CI) discipline. A view held by many in the Defense intelligence community is that CI has not come to grips with these changes, and is out of step with the changes taking place elsewhere in the national and Defense intelligence communities. In fact, CI has been undergoing significant transformation since the 1970s. Each stage in that transformation has produced a greater sense of unity of purpose and commonality of objectives in the CI community. The Defense CI community is also actively adapting to these profound environmental changes that have taken place since 1986. Much remains to be done, however, in terms of defining the desired end state for jointness in Defense CI, and in mapping the most appropriate path to that end state. Defense CI faces a number of important strategic challenges in the years ahead. A key element in evaluating these challenges is finding the correct balance between CI support to joint and unified military operations on the one hand, and continued CI support to the sustaining base on the other. From a careful analysis of these challenges,

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	(over)

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE (*Include Area Code*)	22c. OFFICE SYMBOL
JOSEPH M. BLAIR III, COL, MI	717-245-4404	AWCAC

DD Form 1473, JUN 86 *Previous editions are obsolete.* SECURITY CLASSIFICATION OF THIS PAGE

one may then derive at least the outlines of a desired end state. The question then becomes one of determining what, if any, structural changes need to take place to arrive at the end state. To assist in this determination, this study offers four structural models, each with a different center of gravity, for consideration. This study also offers a framework for further research and discussion on the future of change in Defense CI, and concludes that some change in structures may be inevitable. If Congress or some other external agent drives that change, the result may be less satisfactory than if the Defense CI community sets its own agenda for change.

USAWC MILITARY STUDIES PROGRAM PAPER

JOINT INTELLIGENCE IN A CHANGING DEFENSE ESTABLISHMENT:

THE CASE OF COUNTERINTELLIGENCE

AN INDIVIDUAL STUDY PROJECT

by

Ted R. Snediker
Army Civilian

Colonel Joseph M. Blair, III
Project Adviser

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Ted R. Snediker, Army Civilian

TITLE: Joint Intelligence in a Changing Defense Environment: The Case of Counterintelligence

FORMAT: Individual Study Project

DATE: 22 March 1993 PAGES: 58 CLASSIFICATION: Unclassified

The reexamination of Defense intelligence roles, functions and organizational structures stimulated by the Goldwater-Nichols Act of 1986 and subsequent changes in the global and fiscal environments includes the counterintelligence (CI) discipline. A view held by many in the Defense intelligence community is that CI has not come to grips with these changes, and is out of step with the changes taking place elsewhere in the national and Defense intelligence communities. In fact, CI has been undergoing significant transformation since the 1970s. Each stage in that transformation has produced a greater sense of unity of purpose and commonality of objectives in the CI community. The Defense CI community is also actively adapting to these profound environmental changes that have taken place since 1986. Much remains to be done, however, in terms of defining the desired end state for jointness in Defense CI, and in mapping the most appropriate path to that end state. Defense CI faces a number of important strategic challenges in the years ahead. A key element in evaluating these challenges is finding the correct balance between CI support to joint an unified military operations on the one hand, and continued CI support to the sustaining base on the other. From a careful analysis of these challenges, one may then derive at least the outlines of a desired end state. The question then becomes one of determining what, if any, structural changes need to take place to arrive at the end state. To assist in this determination, this study offers four structural models, each with a different center of gravity, for consideration. This study also offers a framework for further research and discussion on the future of change in Defense CI, and concludes that some change in structures may be inevitable. If Congress or some other external agent drives that change, the result may be less satisfactory than if the Defense CI community sets its own agenda for change.

LIST OF ILLUSTRATIONS

Figure		Page
1.	MILDEP-Centric Model	31
2.	OSD-Centric Model	37
3.	DIA-Centric Model	40
4.	Joint-Staff-Centric Model	44

INTRODUCTION

This study will summarize a variety of agents of change that have had impact on the counterintelligence (CI) community since the 1970s, but particularly over the past decade. It will set forth a number of challenges for CI resulting from changes in the global security environment and national strategy. Finally, with these factors in mind, we will construct a framework for further research and discussion in terms of defining a desired end state for jointness in CI in the Department of Defense (DOD), selecting the most appropriate pathway to that end state.

The reexamination of DOD intelligence roles, functions and organizational structures stimulated by the implementation of the 1986 Goldwater-Nichols Act includes CI, but as yet has produced little noticeable change in DOD CI methods or architectures. This statement reflects what appears to be the convent onal wisdom in some quarters of the Defense intelligence community, and reflects a feeling that CI is somehow out of step. CI has been and continues to be primarily under the direction and control of the service secretaries, a circumstance which has produced a view among some that CI is generally mired in service parochialism. The fact that CI roles and missions in the joint arena remain largely undeveloped is sometimes viewed as resistance to change.

In fact, CI as a discipline has not been standing still. Much has been done and continues to be done within the US intelligence community to improve CI and make it more responsive to national security and defense needs, particularly in the joint operational arena. In mid-1992, the first effort began to develop joint doctrine and tactics, techniques and procedures for CI within DOD. Service CI agencies have become more conscious of the need for a close supporting relationship with components of the combatant commands. Although much progress has occurred, much remains to be done. Among other things, there is as yet no clear vision of an agreed, desired end state for Defense CI in joint terms. It is time to begin serious consideration of that end state.

Few senior officers on active duty today are better qualified to comment on jointness in Defense CI from a strategic perspective than Major General John F. Stewart, Jr., U.S. Army. At this writing, General Stewart serves as the Deputy Chief of Staff, Intelligence, U.S. Army Europe. In recent years, he served as J2, U.S. Southern Command; as Commander, U.S. Army Intelligence Agency; and as G2, U.S. Army Central Command during operations DESERT SHIELD and DESERT STORM. In commenting on jointness in Defense CI, General Stewart wrote:

> T[he] focus on joint operations, coupled with the inevitable reduced resources of the future . . . dictates that CI get on the joint bandwagon. . . . The change will not be easy, but the professionals need to accomplish it so we can serve the nation well or a solution will be dictated to us that will not be in the best interests of the services or the country.[1]

The central issue is thus not just the achievement of some measure of jointness in defense CI, but choosing the proper path to jointness with a clearly defined end state in view. As in many military disciplines, there are many theoretically possible paths to jointness. Devising and designing a path is relatively easy. Selecting and implementing the right path toward the end state is a matter of considerable difficulty.

Authoritative literature on the subject of contemporary CI is scant. Thus the author has drawn to a considerable extent on his own expertise developed out of nearly three decades in military intelligence and over 20 years in CI. For the rest, the author is indebted to a variety of officials in the Defense intelligence community who have contributed their own expert views.

AGENTS OF CHANGE

Changes in the U.S. counterintelligence community have been going on for over a decade. CI, as it is practiced in 1993, is significantly different from the CI we saw in 1981. The net effect of these changes has been to create a CI community out of a set of rather narrowly focused and parochial agencies with little sense of community. Within DOD, these changes have gradually moved the largely decentralized CI community toward a sense of jointness and unity of effort.

Events of the 1970s and 1980s have served both to stimulate change in Defense CI and to shape change toward a sense of jointness. Of these historical episodes, one stands out as providing a sharp focus on both the need for CI and the need for a unity of effort in CI. The "Year of the Spy," mid-1985 to the latter part of 1986, illuminated historical shortcomings in CI, and served to focus the attention of both Congress and the Executive Branch on a program for change.

Year of the Spy. The arrest of John Walker in May 1985, along with his brother, son, and confederate Jerry Whitworth, for espionage on behalf of the Soviet Union produced shock waves throughout the country. The Walker case prompted a great deal of public posturing by elected officials, including President Reagan, various members of both houses of Congress and of both major political parties. Within little more than a month after Walker's arrest, the House of Representatives had rammed through a bill amending the Uniform Code of Military Justice to provide for the death penalty for peacetime espionage acts.[2] The news media brought awareness of the espionage threat to the American public in a major way. To illustrate, the New York Times in 1984, before the Walker case, ran a total of 131 articles on espionage. In 1985, there were 368 such articles, and in 1986, 373.[3] Many of these appeared on the front and "op ed" pages. Beyond exposure of the espionage threat, the recurrent theme of this publicity was criticism of the shortcomings of the country's CI and security apparatus.

The Walker-Whitworth arrests were followed in relatively short order by other sensational espionage arrests which cumulatively produced a staggering degree of damage to national security. A 1986 statement by the Senate Select Committee on Intelligence (SSCI) characterized damage from the Walker case and others as ". . . far greater than anyone in the U.S. govermnent has yet acknowledged publicly . . . billions of dollars of actual and potential damage to U.S. military programs."[4]

The year 1985 thus became known in the popular press as the "Year of the Spy." The wave of espionage arrests did not stop there, however. The U.S. Army had its own "Year of the Spy" in 1988 with the arrests of Clyde Conrad and James Hall. Conrad, a retired U.S. Army non-commissioned officer living in Germany, had for several years been selling classified NATO, V Corps and 8th Infantry Division war planning documents to Hungarian intelligence. These and many other arrests, primarily of U.S. citizens, through the end of the 1980s suggest that rather than a "Year of the Spy", we had a "Decade of the Spy."

One of the ironies of working in CI is that what the CI agent considers to be a significant CI success--the arrest of a spy--is something that non-intelligence leaders in the military and government generally tend to view rather as a security failure. How, they ask, could we have been so badly duped for so long by so many? Moreover, the great majority of the U.S. citizens involved were "insiders", that is, they were military

personnel or U.S. civil servants who had been investigated and cleared for access to classified information. What, these same leaders ask, is wrong with our personnel security system that we do not detect these spies? Why, they continue, did it take CI investigators nearly two decades to detect a John Walker, or one decade to bring down a Clyde Conrad?

Such questions can be answered at length by explanations of the difficulty of detecting and investigating espionage and the inherent imperfections of personnel security investigations which must be accomplished within the framework of our democratic society. The most germane response to these very legitimate questions, however, is that not until the mid-1980s did CI in the US emerge from the dark age imposed on it in the early 1970s.

CI's Dark Age. Public revelations of investigative excesses by the FBI and the military CI agencies--especially the Army's--during the late 1960s and early 1970s produced Congressional outrage and Executive Orders 11905 and 12036.[5] These clearly aimed at reining in what the Administration and Congress alike portrayed as a rogue CI apparatus. The investigations in question were originally stimulated by U.S. Government fears of widespread civil disturbances carried out in the context of the civil rights and anti-Viet Nam war movements. Outbreaks of violence had become commonplace, and reached a zenith of sorts in the wake of the assassination of Martin Luther King in April 1968, which touched off riots necessitating the use of federal military resources to restore order.

Neither the White House nor the military had much experience or expertise in dealing with such phenomena, and the distinctions between lawful dissent and unlawfully violent dissidence were not well understood. In an effort to gain a better understanding of the sources of civil violence, the Johnson Administration and DOD deployed the FBI, other law enforcement agencies, and the military CI agencies as an intelligence force. These agencies pursued their intelligence mission with a great deal of zeal but little oversight or guidance on what might be termed "rules of engagement." Consequently, the intelligence effort got out of hand, and extended well into the area of mounting clandestine surveillance activities against virtually anyone who was perceived to support these movements.

Regulatory guidelines implementing the Executive Orders within DOD[6] were even more draconian than the orders themselves. The excesses had besmirched the reputation of the military, particularly the Army. Individuals and groups involved in the protest movements who had learned that they were targets of such intelligence activities inundated DOD and senior officials with litigation. The mood of leaders in DOD was that CI must be gotten under control. The control that ensued, most in the CI community would agree, virtually paralyzed legitimate CI investigative and operational efforts.[7]

This paralysis, in turn, produced institutional atrophy in the service CI agencies, and over time the kinds of skills needed to conduct CI activities against sophisticated opponents were

largely lost. This "Dark Age" for CI was unquestionably a major contributing factor to the ability of the John Walkers and the Clyde Conrads of the world to carry out their treasonous activities for long periods of time, undetected.

In a more positive vein, CI's Dark Age did produce a greater awareness in Defense CI of the legal framework within which it is obliged to operate. Moreover, during the Dark Age, CI professionals had the time to reflect while seeking meaningful work, and a consensus began to grow that traditional CI, which was largely limited to counterespionage, did not capture the total nature of the threat. They began to see that many countries, and especially the Soviet Union, had well developed, sophisticated intelligence capabilities that paralleled those of the U.S. signals intelligence, imagery, and other intelligence capabilities were part of that package, and needed CI's attention. Further, there was a dawning realization that intelligence threats were not limited to those of our avowed enemies. Prudence dictated that there should be some level of concern about the intelligence services of many countries. These included non-hostile countries who wished to acquire more information about the U.S. than the U.S. wished to share, as well as a number of states with whom the U.S. could become embroiled in a contingency situation.

Two key CI concepts arose from this thinking which ultimately contributed to greater dialogue and a sense of common purpose among the Defense CI agencies. First was the notion that

CI's mission was to deal with intelligence threats generally, and thus came into being the concept of a multi-discipline approach to CI which would take into account the whole range of activities carried out by intelligence services. The second was that while the highest priority for CI was the aggregate of so-called hostile intelligence services, there was a need to deal in some fashion with the larger problem of foreign intelligence services generally.

These concepts later proved to be a sound basis for transitioning from the terrible certainties of the Cold War era into the uncomfortable uncertainties of the emerging New World Order. More immediately, however, the acceptance of these concepts by the various CI agencies, coupled with the relatively new understanding that each agency could in its own way enhance the knowledge and understanding of the others, led to increasing dialogue and sharing of data. The analytical elements in the CI agencies especially became a significant stimulus to a growing sense of community among the CI agencies and to a resultant sense of jointness on an interagency level.

Rehabilitation and Renaissance. If the 1970s were CI's Dark Age, then the 1980s proved to be its Renaissance. In 1981, a new Executive Order, EO 12333,[8] on U.S. intelligence activities reflected a change in the way both the Administration and Congress viewed the importance of intelligence activities generally. The new Reagan Administration was pursuing an announced policy of dealing with what came to be called "The Evil

Empire", and a vigorous intelligence capability, to include CI, became an important arrow in the President's quiver. The political rehabilitation of CI had begun. From that point, CI began to experience a recovery from its Dark Age, and by the mid-1980s had recovered its lost talents sufficiently to begin to experience success in ferreting out spies. In his first public commentary on the subject, President Reagan ". . . called for overturning 'unnecessary restrictions on our security and counterintelligence officials' that were imposed during the 1970s.[9] Later, the President stated in one of his regular Saturday radio addresses that the Administration had given a high priority to combatting espionage.[10]

The Year, or Decade, of the Spy brought home to leaders in Congress, the Administration and DOD the importance of effective CI and security countermeasures to national security, and created a climate of fiscal and policy support for further improvements. It also brought home to the CI community that interagency cooperation toward a common purpose was essential. In 1986, the SSCI issued a report that was highly critical of CI and security, and accused the various agencies involved of less than full cooperation. Most importantly, it called for the creation of a national CI strategy that would, among other things ". . . integrate the planning and resources of the various agencies . . . ."[11] In fact, many of the CI successes of the late 1980s resulted from close interagency collaboration. As the various CI agencies became more accustomed to dealing with one another

routinely, they learned that they could produce much synergy by taking advantage of the sometimes unique capabilities of the other agencies.

By the late 1980s, and before the fall of the Berlin Wall signaled global political change, CI was showing signs of a full recovery from the Dark Age of the 1970s, and making significant inroads into countering the threat posed by hostile intelligence services, especially those of the Soviet Union and its Warsaw Pact allies. The ensuing collapse of communism, the Soviet Union and the Cold War produced much the same effects of rethinking and reorientation on the CI community as it did on the rest of the intelligence community and the national security structure generally.

As a result of the 1986 SSCI report, the National Security Council (NSC) and the Director of Central Intelligence (DCI) began to play an active role in solidifying the CI community and creating unity of effort to a significant degree. Under the NSC and DCI aegis, the CI community prepared a strategic, interagency approach to CI in response to National Security Review (NSR) 18. The NSR 18 report was in final form when the tide of political upheaval began in Eastern Europe. There was a fast-paced reevaluation and rewrite of NSR 18 to accommodate the new realities, and President Bush ultimately approved the new national CI strategy in the form of National Security Directive 47 in October 1990.[12]

The interagency mechanism that undertook the formulation of the NSR 18 report was the already existing Senior Interagency Group/Intelligence (SIG/I), with its subordinate interagency groups (IGs) for CI and security countermeasures. The Director of the IG/CI was the FBI Director, Judge William Webster, who later became the DCI. Under Judge Webster's leadership, the IG/CI began to flourish as the primary agent of change in the CI community. During the Bush Administration, the National Advisory Group for CI and Security Countermeasures (NAG/CI&SCM) replaced the SIG/I, and a set of Advisory Groups (AG) for CI and Security Countermeasures replaced the IGs. At about the same time, Judge Webster became the DCI.

William Sessions, who replaced Judge Webster as FBI Director, brought into being two subgroups under the AG/CI, the CI Operations Board (COB) and the Policy Steering Group. The role of the latter was primarily the identification of CI policy issues to be placed on the AG/CI agenda. It was the COB, however, that truly infused the CI community with unity of purpose and action in a meaningful and concrete way.

The COB came into its own shortly after the fall of the Berlin Wall in late 1989. Originally created to provide Director Sessions with a "fast-track" capability to review and make recommendations on community CI issues, the COB quickly became the leading edge in evaluating the significance for CI of the global political upheaval that was beginning to take place and

taking deliberate and coordinated operational steps to deal with those changes.

The military service CI agencies, as well as OSD, were active players in the COB from the beginning. Although the "jointness" embodied in the AG/CI and its COB was at the national Intelligence Community level, it had its impact on the interservice level in DOD as well. Through the COB, senior operations officers from the service CI agencies had a meaningful and substantive forum that met with a frequency and intensity likely never before experienced.

The Sense of Congress. The political rehabilitation of CI also extended to the halls of Congress during the latter half of the 1980s. The atmosphere of both the House Permanent Select Committee on Intelligence (HPSCI) and the SSCI had changed dramatically since the 1970s. From the perspective of Congressional oversight, the attitudes of both committees had become benign and seriously concerned about enabling the CI agencies to do a more effective job. In budgetary matters, their attitude became beneficent and generous. CI benefitted along with the rest of the Intelligence Community and Defense in gaining resources desperately needed for modernization.

The budgetary gravy train began to slow to a stop more than a year before the fall of the Berlin Wall, however. The demands of the Gramm-Rudman-Hollings Act for a balanced Federal budget brought budgetary growth for CI to an end. The end of the Cold War and demands for a peace dividend which began the large scale

downsizing of the military affected the Intelligence Community and its CI component as well. In the 1990s, CI has experienced cuts in both manpower and dollars that parallel the magnitude of overall defense cuts. The effect has been to cut off CI modernization in mid-stream.

Fiscal decline notwithstanding, the Congressional committees have thus far remained supportive of CI in a policy sense, and have conveyed a sense of satisfaction with the direction the CI community has been heading. In February 1992, the Chairmen of the SSCI and HPSCI, Senator David Boren and Congressman Dave McCurdy, introduced companion bills intending to produce wide-ranging reorganization of the U.S. Intelligence Community to accommodate both fiscal reality and global political change. CI was conspicuous by its absence of mention in either bill. For his part, Senator Boren indicated that this was a deliberate omission,[13] signifying that the existing framework for CI in the Intelligence Community was satisfactory.

In reaction to the proposed Boren-McCurdy bills, the then Director of Central Intelligence, Robert Gates, proposed, received Presidential approval,[14] and quickly implemented his own version of intelligence community reorganization in an effort to finesse the need for legislation. Like Boren-McCurdy, however, Gates left CI alone. Thus, the CI community seemed to have had both its structure and strategic direction validated by both the Congress and the Administration. There has been, of course, since those events the inauguration of a new Administration and

the seating of a new Congress. How the Clinton Administration, the new Director of Central Intelligence, the new Secretary of Defense and new sets of Congressional eyes may view the CI community is still an open question at this writing.

DOD Internal. The impact of the Year of the Spy and the resulting Presidential and Congressional pronouncements cascaded down to the DOD level even more so than to the Intelligence Community. DOD, after all, was the governmental entity most affected by the Year of the Spy.

In reaction to that event, Secretary of Defense Caspar Weinberger in 1985 created the Stilwell Commission to examine the state of security generally within DOD and to offer recommendations for improvement. Subsequent experience in providing CI support in joint military operations provided important lessons to the Defense CI community. Toward the end of the 1980s, Defense CI began to feel the impact of the Goldwater-Nichols Act in terms of the strengthened roles of the CINCs, the CJCS and the Joint Staff.

Concurrently, the consolidation of intelligence and security functions under the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD[C3I]) and the creation of the office of the Deputy Assistant Secretary of Defense for CI and Security Countermeasures (DASD[CI&SCM]) provided the staff coherence necessary to undertake a comprehensive review of Defense intelligence generally, to include CI.

On 25 June 1985, little more than a month after John Walker's arrest, Secretary Weinberger established the DOD Security Review Commission under the direction of retired Army General Richard G. Stilwell. What became generally known as the Stilwell Commission included Under Secretary Fred Ikle; three Assistant Secretaries of Defense; the DOD General Counsel; the Directors of the Army Staff, Naval Intelligence, the National Security Agency, and the Defense Intelligence Agency; the Inspector General of the Air Force, a retired Navy admiral, and the Director of Security for E. I. DuPont deNemours & Co.[15]

The Stilwell Commission's report, Keeping the Nation's Secrets, was issued on 19 November 1985. It contained a total of 63 recommendations for enhancing security within DOD, of which Weinberger approved slightly more than 50. According to the former assistant to the Army Commissioner, the primary thrust of the Commission's work and its report was in the area of security countermeasures rather than CI. There were, however, linkages to CI such as the expanded use of the polygraph as a security screening tool which influenced the development and refinement of various DOD policy issuances on CI.[16] The Commission's report also directly influenced community level deliberations on NSR 18. In sum, it did much to provide focus for the developing sense of unity of effort among the Defense CI agencies.

Perhaps the first significant development toward a joint approach to CI in military operations was the concept of assigning CI Staff Officers (CISOs) to each Unified and Specified

(U&S) Command headquarters. The idea was born in mid-1987 as a result of another experiment in joint CI, the Joint CI Operational Element (JCIOE).

The U.S. Southern Command created the JCIOE in the mid-1980s to provide CI support to Joint Task Force Bravo (JTF-B) in Honduras. JTF-B arose from the buildup of U. S. military support to Honduras that began around 1973.[17] Its mission became one of coordinating the U. S. force presence there involved in training, contingency planning and support, and nation building.[18] The original concept for JCIOE was to bring elements of the Army's 470th Military Intelligence Brigade, based in Panama, and of the Air Force Office of Special Investigations (AFOSI) Miami regional office under the command of the JTF-B commander.

By 1987, this novel command and control relationship had begun to cause problems with the Army, and to some extent, with the Air Force. The issues were two: doctrine and oversight. While Army intelligence and AFOSI had worked together cooperatively for many years, they were fundamentally different types of organizations with greatly differing doctrine and operating rules. AFOSI is fundamentally a law enforcement organization. It operates primarily under criminal investigations guidelines, and only to a limited extent under intelligence guidelines. Army CI, as part of Army intelligence, is an intelligence component, and operates solely under intelligence guidelines. These differences largely manifest themselves in the accountability and approval levels for various

kinds of operational activities, and to some extent in techniques and procedures. Establishing a mutually acceptable standing operating procedure under these circumstances was at best difficult. Oversight, a parent service responsibility, also became a problem under the unusual command relationship established for JCIOE.

When the JCIOE situation came to the attention of the then Director of CI in OSD, John Donnelly, he concluded that the problem arose in large part because there was no experienced CI officer assigned to the CINC's staff. This proved to be generally the case among U&S commands. After a round of consultations with the CINCs, Donnelly directed his staff to prepare a policy issuance that would provide each CINC with CI expertise on his staff in the form of a CISO, and at the same time provide the theater CINCs operational control of CI elements during military operations.

The result was DOD Instruction 5240.10, "DOD Counterintelligence Support to Unified and Specified Commmands," published in May 1990.[19] This was the first official DOD pronouncement on jointness in Defense CI.

By the time of the DESERT SHIELD deployment in August 1990, most U&S commands had identified a CISO. The CISO concept and the new DOD Instruction received their acid test during DESERT SHIELD and DESERT STORM. They appeared to work well and as intended. Most importantly, this seed of jointness in CI had

sprouted and taken root in the framework of joint military operations.[20]

Within the Pentagon, other developments in OSD that were more or less concurrent with the Gulf War would provide the next major increment of jointness in Defense CI. Policy and programmatic responsibility for CI and security countermeasures shifted from the Deputy Under Secretary for Security Policy to the Assistant Secretary for C3I, Duane Andrews. This change came at a time when it had become apparent that the size of the Defense establishment was going to be reduced significantly and that the Cold War Era was coming to an end.

One of Andrews's first tasks was to develop a scheme for broad restructuring and refocusing Defense intelligence to accommodate the new realities. The plan emerged in March 1991 in the form of a memorandum signed by Defense Secretary Dick Cheney entitled "Plan for Restructuring Defense Intelligence."[21] The tone and direction this memorandum set produced two additional steps toward jointness for Defense CI: the development of a DOD CI strategy document and the creation of a Joint CI Support Branch to support the Joint Staff J2.

When Andrews assumed the CI and security countermeasures function, a political appointee, Nina Stewart, filled the newly established post of Deputy Assistant Secretary for CI and Security Countermeasures. During her tenure, she was responsible for developing the "Counterintelligence Strategic Plan for the 90s," issued in white paper form on 1 December 1992. This paper

does not tie directly to the March 1991 memorandum, but clearly reflects its spirit, as well as that of DCI Gates's efforts to reorient the Intelligence Community generally. While the CI plan is a classified document, some of the more pertinent portions are unclassified. Most relevant are the vision statement it contains and two specific objectives:

> THE VISION
>
> The DOD CI program must detect and deter foreign intelligence efforts to compromise our Nation's defense capability. Defense CI will work closely with the SCM community to ensure a rational development of protection for critical weapons systems, both classified and unclassified sensitive technological data, and critical resources. Key to these efforts will be the maximum exchange of critical CI information between intelligence community members to ensure timely CI participation in the identification, characterization and neutralization of threats. Integrated CI and SCM support for both policy makers and Combatant Commanders is, and will continue to be, a top priority. Future Defense CI efforts will reflect a commitment to providing a quality product responsive to the needs of our consumers.
>
> SPECIFIC OBJECTIVES
>
> Improve CI responsiveness to the needs of the services and Combatant Commanders, especially in the execution of contingency plans, through the integration of CI into the overall planning process; ensure the effectiveness of the Joint Counterintelligence Support Branch in support of the Joint Staff in the Pentagon and the Counterintelligence Staff Officers at Unified and Specified Commands.
>
> Enhance the effectiveness of the current CI organizational structure. Where appropriate, centralize functions to reduce duplicative staffing. Organizational structures must support needs of the military departments and Combatant Commanders, while reinforcing military service management of CI.[22]

STRATEGIC CHALLENGES FOR DEFENSE CI

The DOD CI Strategic Plan set forth a number of challenges for Defense CI in the years ahead. Analysis of these, particularly in the light of prospects for diminished CI resources, shows among other things that there is now a fairly clear demarcation of CI support to the combatant commands on the one hand, and support to the sustaining base on the other. In the latter category, of particular concern is the Defense research, development and acquisition community. A key element in evaluating strategic CI challenges, then, is finding the correct balance between a proper and properly joint approach to supporting the combatant commands on the one hand, and continued support for the sustaining base on the other. The challenges set forth here are not those of the Strategic Plan, but rather of the author's own devising.

CI Support to Combatant Commands.

In supporting the combatant commands, the challenge is primarily one of defining what joint requirements for CI are to be and ensuring that the services and DIA are properly structured to meet those. The Joint Staff J2 is now positioned to take the lead in ensuring the incorporation of relevant CI considerations into joint planning and doctrinal development.

A Chairman of the Joint Chiefs of Staff (CJCS) memorandum to the Joint Staff in 1992 established the CI role of the J2 and

requires that there be CI review and input in all aspects of the Joint Strategic Planning System.[23] A salient challenge for both the Joint Staff J2 and the service CI Liaison Officers working with the Joint CI Support Branch will be to use this voice in developing a practical means of compensating for the loss of continuity in forward presence as our military forces become increasingly CONUS-based.

In common with other intelligence disciplines, particularly human source intelligence (HUMINT), CI incurs a distinct disadvantage from the emphasis on force projection as opposed to forward basing. Successful CI operations depend to a significant extent on presence in a given area of operations in advance of any response to a contingency. Area knowledge, language, and host country agency liaison are essential elements that are not continuously available to CI elements that remain for the most part in CONUS.

For contingency deployments, CI might seek to use commercial transportation or influence the Time-Phased Force Deployment Document system at the Joint Staff level by getting CI to the theater of war as early as possible. General Stewart commented:

> The key is to get CI elements in early. . . . There is much early work to do concerning CI liaison with host country intelligence and security organizations, establishing source networks, coordinating reporting procedures, conducting threat assessments, conducting liaison with the U.S. embassy for security purposes, and establishing contact with UN and multinational staffs.[24]

CI could also seek to integrate itself into the CJCS concept of Adaptive Joint Force Packages[25] as a means of gaining and preserving experience in forward presence areas.

Command Intelligence Architecture Plans (CIAPs) generated by the combatant command staffs have generally begun to consider the commands' CI requirements. As these evolve, the challenge for CI elements supporting or assigned to the service components and the components' staffs themselves will be to work closely and cooperatively with the CINC's staff to ensure that an appropriate balance is struck between unified effort at the combatant command level and continued support to the respective components. In addition, component CI elements will be challenged to learn how to play effectively in the JSPS at the combatant command level as an extension of the challenge to the Joint Staff and military departments outlined above.

In mid-1992 began the first effort to develop joint doctrine, tactics, techniques and procedures for CI. At this writing the effort has already born fruit in the form of a draft Joint Publication 2-03.[26] The existing test Joint Publication 2-0, Doctrine for Intelligence Support to Joint Operations,[27] largely ignores CI. Joint Publication 2-03 will redress this deficiency to a large extent.

The key challenge and the key opportunity for CI in developing joint doctrine will be to provide value added to the combatant commanders through a doctrinal formula that will produce true unity of effort among the various agencies. The

service CI agencies must remain responsive to service unique requirements, but there is no place in the process for service parochialism.

Two of the most important issues embedded in this challenge are defining CI command and control relationships and developing a clear CI role in unified command intelligence processes. Without the right set of command and control relationships linking headquarters and components, unity of effort in military operations will be no more possible for CI than for any other discipline. The Army Staff's Director of CI and SCM believes that the eventual role of CI in the theater Joint Intelligence Centers, and how that role is defined, will be a crucially important test bed for emerging joint CI doctrine.[28] This view is likely correct, in that among the four major CI functions, intelligence production most readily lends itself to jointness. Service level doctrine on the CI production function is fairly uniform as it is, and much more so than on the CI investigative function, for example.

CI Support to the Sustaining Base.

The focus of Defense CI support to the sustaining base must be congruent with national security and military strategies. This applies most especially in technological areas having to do with superior, sophisticated defense systems that will continue to provide our smaller forces with a compensating technological edge. CI will face further challenges in the general areas of

technology transfer, special weapons proliferation and arms control.

Protecting the technological edge. It is generally accepted that CI has a role in force protection. An important, if indirect, way CI contributes to force protection is by aggressive support to the protection of technologies we will put on the battlefield in the years ahead. The challenge to CI will be to develop efficient methodologies for this type of support under a broadly based effort such as the Acquisition Systems Protection Program.

Special weapons proliferation and arms control. Since the ratification of the Intermediate Nuclear Forces Treaty, CI has learned a good deal about the prevention of the unintended loss of technological information in the context of intrusive on-site inspections. On-site inspections has become a normal means of arms control treaty verification. Success in this area will continue to challenge CI. The new challenge will be to develop similarly successful methodologies to support strategic objectives to limit the proliferation of weapons of mass destruction.

Other CI Challenges.

There are also a number of challenges which transcend questions of support to combatant commands and the sustaining base. These issues have service as well as joint implications.

Transitioning from an environment that was clearly threat based to the more ambiguous, capabilities based environment the U.S. faces generally poses challenges for CI as well as for other functions related to national security. The national level CI community has already done much work in this area in the context of the AG/CI, and the conclusion has been in general terms that there remains a set of what has been termed traditional threats emanating from such countries as Russia, China, North Korea and Cuba. Beyond these, there is also a set of "non-traditional" threats. These focus on issue areas of national concern (e.g., special weapons proliferation, technological superiority, economic competitiveness) in which the U.S. may face intelligence threats from a variety of countries, to include some which are at least nominally friendly to the U.S..

While this approach is useful and in tune with the times, it does not account for intelligence threats which may not be present or identifiable until a military deployment is ordered. The challenge for Defense CI will be to anticipate and prioritize carefully and correctly the appropriate set of intelligence threats on the one hand, and to posture itself with the appropriate capabilities to deal with issue area type threats that do not lend themselves to prediction.

Rapid technological advances in information handling, both in terms of communications and automation, present new and potentially very lucrative opportunities for foreign espionage and sabotage. CI agencies at the national level as well as

within DOD must jointly and continuously develop and refine advanced investigative techniques to enable the detection of such activities.

Finally, there is something of an identity crisis that has been emerging for CI since about 1990, and it begs resolution. Within the realm of intelligence and security, CI often finds itself as something of a "loner." It is a unique activity, but one which is interlocked with other disciplines.

Within the CI community generally, there are two schools. One of these, exemplified by the CIA and followed by DIA and the Army, views CI primarily as an intelligence discipline. The other, to which the FBI, the Navy and the Air Force adhere, sees CI primarily as an aspect of law enforcement.

The Army, the Marine Corps, and to some extent OSD and DIA, also see a strong affinity between CI and HUMINT. In Army Intelligence, CI and HUMINT have a long historical relationship and are functionally intertwined, especially at operational and tactical echelons. In combat intelligence operations, the two are sometimes virtually indistinguishable.

On the other hand, CI has a very close, inherent relationship with the security countermeasures disciplines. The NAG(CI&SCM) structure at the national level under the DCI, as well as the creation of the DASD(CI&SCM) in DOD under the ASD(C3I) reflect the legitimacy of this relationship.

Those in Congress and DOD who are rightly seeking ways of achieving greater efficiencies and economies may well seek to

merge CI with one or another of these. Alternatively, as has happened in the past, there could be a move to consolidate criminal investigative functions, less CI, at the DOD level, thus removing that function from the services. That raises the question of what to do with the CI elements in the Air Force and Navy, which are part of their respective criminal investigations agencies. Whether in a mode of self-defense against institutional tinkering or simply to impart a clearer sense of self-identity, the Defense CI community needs to address the issue in a joint fashion.

The strategic challenges for CI abound with opportunities for unified effort among the services. Indeed, a joint approach to these may well prove to be the main key to success in meeting these challenges. The institutional path to jointness in Defense CI is another matter entirely.

PATHS TO JOINTNESS: FOUR MODELS

Unquestionably, jointness has become the primary byword in DOD since the passage of the Goldwater-Nichols Act in 1986. Much of this paper thus far has focused on how CI within DOD has gradually edged itself toward a sense of community, and hence, jointness, in the approach that this essentially decentralized discipline takes in fulfilling its role and accomplishing its functions. That sort of jointness has centered around increasing dialogue, coordination, data sharing and the like. Defense CI is

now approaching the formulation of joint doctrine, but there has not been much serious consideration so far of a general restructuring of CI within DOD. It may prove neither necessary nor desirable to do so, but some serious consideration of options seems timely and appropriate.

There are many paths to jointness. Centralizing resources into a "purple suit" organization either at the DOD or U&S command level may appeal to some, but it is by no means the only way to achieve an adequate degree of unity of purpose and action, which is really at the heart of jointness. It may well be that a coherent body of joint policy, doctrine, and procedures, coupled with consistency and determination in coordination and collaboration among the DOD CI agencies is sufficient.

Even so, it is perhaps time to give some consideration as to what alternative structural models there might be for CI within DOD. Some work in this area was done in mid-1992 by the office of the DASD(CI&SCM) in response to perceived pressures from Congress to consolidate criminal investigations functions in DOD, and in particular from the HPSCI to create some sort of DOD-level CI agency as a means of consolidation of resources. This effort never went beyond the discussion stage, but it did at least set forth a set of five models, along with their attendant advantages and disadvantages, for consideration.[29] This set of models excluded the *status quo*, and for the most part focused on combining CI with an existing Defense agency. For purposes of this paper, and absent external pressures to do so, we will

propose, examine, and subsequently analyse, a different set of four alternative models.

MILDEP-Centric Model: ("Service CI Agencies").

This model represents the present-day status quo. The OSD set did not consider this model, since it assumed that there would be some form of Congressional pressure for change from the status quo. It nevertheless provides a baseline for comparison with the three alternative models. Under this model, the primary authority and responsibility for the conduct of CI investigations and operations is vested in the secretaries of the military departments (MILDEPs). This reflects their current responsibilities under Title 10, U. S. Code,[30] as well as over five decades of organizational evolution in which the CI agencies of each service has been shaped to conform to the needs of the respective MILDEPs.

As can be seen in Figure 1, there is significant diversity in the way CI is structured in the three MILDEPs. In the departments of the Navy and Air Force, CI has been structured primarily as an adjunct function of the MILDEPs' criminal investigation agencies: the Naval Criminal Investigative Service (NCIS) and the Air Force Office of Special Investigations (AFOSI).

There are some important differences, however. AFOSI reports directly to the Air Force Inspector General, is the sole CI actor in the department, and is a fully stovepiped

MILDEP-Centric Model

"Service CI Agencies"

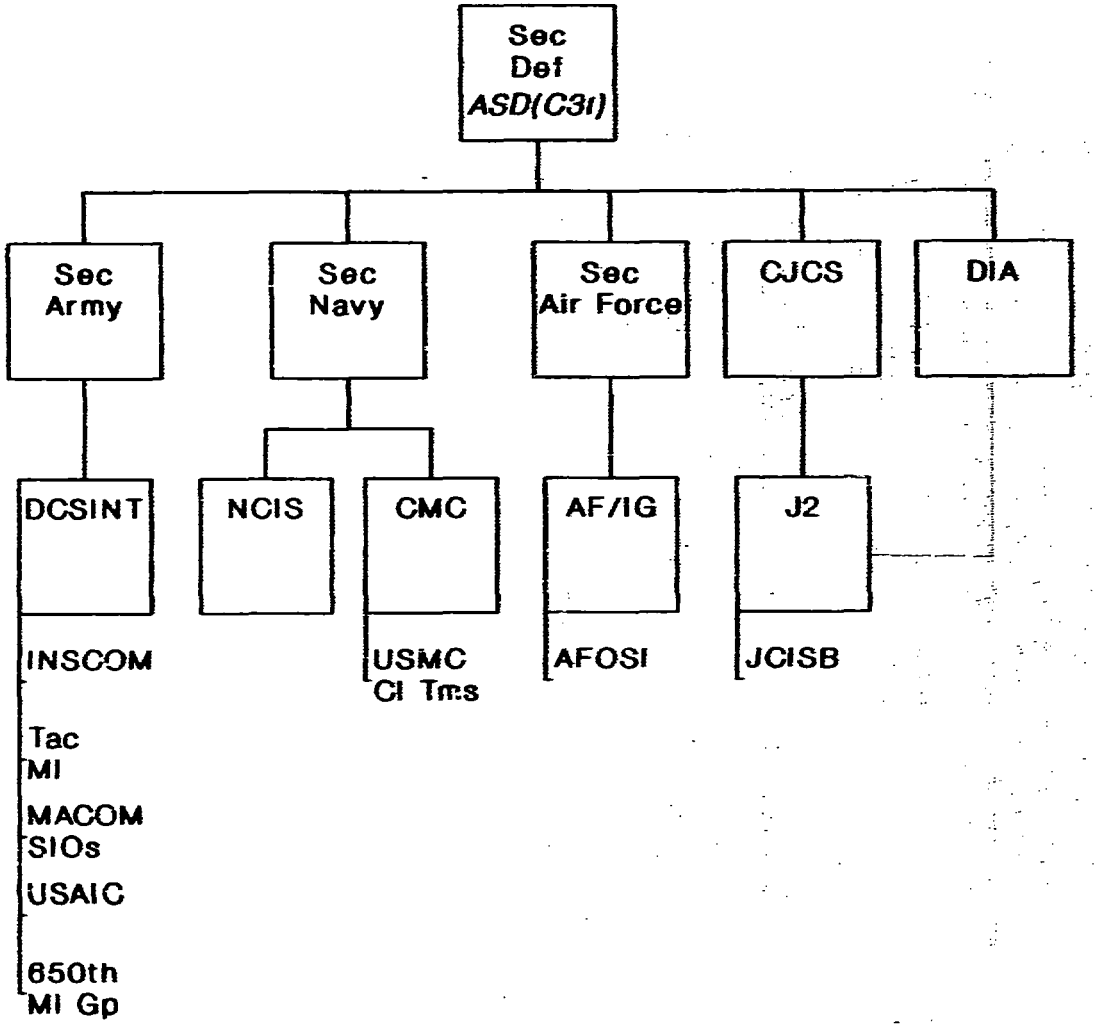

Figure 1. MILDEP-Centric Model

organization. Of the three services, the Air Force has the simplest and most straightforward CI structure.

NCIS is structured internally somewhat like AFOSI to the extent of being a stovepipe organization with a dual criminal investigative and CI mission, but it reports to the Secretary of the Navy through, and takes CI policy guidance from, the Director of Naval Intelligence. Also unlike the Air Force, the Department of the Navy has a number of Marine Corps CI teams which are provided to deploying Marine combat formations for CI support during military operations. These Marine CI teams resemble in most respects the CI elements found in Army MI brigades and battalions at corps and division echelons.

Army CI structures are far different and more complex. The primary divergences between the Army and the other services are two: the Army views CI primarily as an aspect of intelligence work rather than criminal investigations, and the Army does not have a highly centralized, stovepipe structure like the other services. Rather, the Army relies on a network of "control offices" to provide a measure of centralized technical control and coordination of CI investigations and operations, and otherwise leaves the day-to-day management, command and control of CI elements to diversified chains of command in the field.

Atop the Army's CI structure is the Deputy Chief of Staff for Intelligence (DCSINT), the Army's senior intelligence officer and a principal staff officer on the Army Staff. The DCSINT, who reports directly to the Chief of Staff of the Army, functions in

a stewardship capacity for the Secretary of the Army in the discharge of the latter's Title 10 responsibilities for CI and military intelligence activities generally. As the formulator of CI policy for the Army as well as its primary resource manager, the DCSINT provides staff guidance and direction for the conduct of CI activities in the Army generally, but commands no operational CI units. As the Army Staff's "G2", the DCSINT is also responsible for keeping the Army leadership informed of significant CI events and activities impacting on the security of the Army.

Most Army CI resources are vested in the Army's Intelligence and Security Command (INSCOM), which functions under the staff supervision of the DCSINT. INSCOM commands specialized CI units and multi-disciplined military intelligence brigades which deploy with the Army's combat forces. In the latter circumstance, CI elements of the MI brigade are placed under the operational control of the theater Army commander, generally through the command's senior intelligence officer. INSCOM also manages, on behalf of the DCSINT, the system of control offices mentioned earlier.

The DCSINT's authorities and responsibilities for policy guidance and resource management also extend to other Army commands involved in CI. These would include the senior intelligence officers in Army major commands (including the Army component commands at theater level); the Army Intelligence Center and School, a major subordinate command of Training and

Doctrine Command; the 650th MI Group, which provides CI support to Allied Command Europe and reports to the SACEUR; and the MI units and staffs organic to Army corps, division, armored cavalry regiments, separate brigades and special forces groups.

All three MILDEPs share in their CI programs the focus on the departmental secretary (or his designee) as the primary decision maker. The MILDEP secretaries, in turn, report to the Secretary of Defense, who, under Title 10 authority, delineates the specific scope of the MILDEP secretaries' responsibilities for intelligence matters, to include CI.[31] The implication here is that at the OSD level, CI is treated as an intelligence matter, irrespective of MILDEP organizational alignments. Within OSD, CI is aligned to the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD[C3I]), and specifically to the Deputy Assistant Secretary of Defense for CI and Security Countermeasures (DASD[CI&SCM]).

The role played by the DASD(CI&SCM) is roughly analogous to that played by the Army DCSINT: policy, resource management, and keeping the Secretary of Defense informed of significant matters. The DASD(CI&SCM) generally does not become involved in the coordination and decision making processes associated with CI investigations and operations, but may exert operational management by exception where and when required. Examples of this type of management by exception would include tasking the services for CI support in connection with a request for

assistance from the FBI or CIA, or mounting a CI operation in support of a Defense agency or institute.

The DASD(CI&SCM) is also the primary DOD representative on interagency fora related to CI, and chairs the Defense CI Board which fosters interservice and interagency coordination, cooperation, interoperability and data sharing. Finally, the DASD(CI&SCM) may assign to one or another MILDEP executive agency responsibility for CI support to the various defense agencies.

The Defense Intelligence Agency (DIA), whose director reports directly to the Secretary of Defense, has a unique and evolving role in CI. DIA does not have a charter to conduct CI investigations and special operations, but does have a primary role in CI production within DOD as part of its overall general military intelligence production mission. More recently, DIA has constituted for the Chairman of the Joint Chiefs of Staff a J2 directorate, which includes a Joint CI Support Branch (JCISB), established in March 1992.[32]

The JCISB provides the usual kinds of staff action support within the Joint Staff, among several other functions. Most notably to date, JCISB has assumed the role of insuring the infusion of CI considerations into the Joint Strategic Planning System; become the focal point for the development of joint CI doctrine, tactics, techniques and procedures; and has developed a coordinating network among the CI Staff Officers in the U&S

Commands as well as an interservice Joint CI Issues Working Group.[33] The JCISB exerts no authority over service CI elements.

OSD-Centric Model: ("The Defense CI Agency [DCIA]")

The first of the three models to be presented in this paper as possible alternatives to the status quo for structuring CI within DOD posits a major shift in the Title 10 responsibilities of the Service Secretaries with respect to intelligence activities. It assumes that the Secretary of Defense has relieved the Service Secretaries from both the mission and responsibility to conduct and oversee CI investigations and special operations within the military departments. To replace the service CI agencies, this model further assumes that the Secretary of Defense has received Congressional authority to create a new defense agency, to which we will give the notional title of the Defense CI Agency (DCIA).

The DCIA would be structured generally along the lines of the existing Defense Investigative Service (DIS), and, like DIS, would be subordinated to the ASD(C3I) through the DASD(CI&SCM). Also like DIS, DCIA would be headed by a career Senior Executive Service member (or, alternatively by a two-star general or admiral). OSD would task the MILDEPs to provide civilian spaces and military manpower to staff DCIA, which would receive its funding from the Foreign Counterintelligence Program, a component of the National Foreign Intelligence Program managed by the Director of Central Intelligence.

OSD-Centric Model

Defense CI Agency

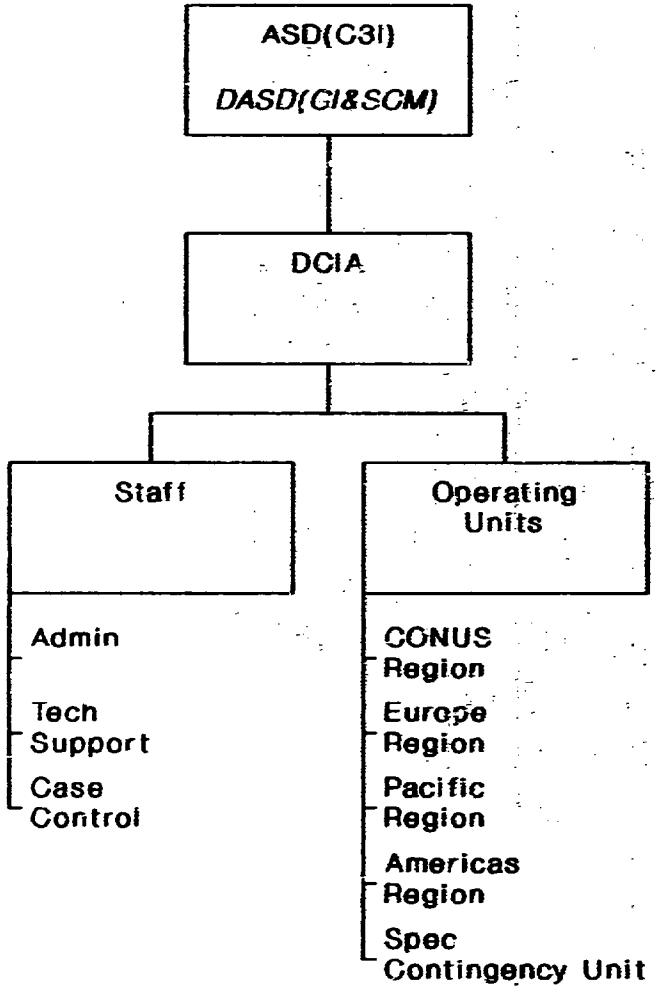

Figure 2. OSD-Centric Model

DCIA would control and conduct all CI investigations and special operations within DOD, and would be the sole point of contact within DOD for operational coordination with FBI and CIA. DCIA would have the additional mission of providing general CI operations support to the U&S commands and defense agencies in the form of security advice and assistance. The existing CI Staff Officers assigned to the U&S commands would be provided by DCIA rather than by the services, as is presently the case.

DCIA would not, however, assume the CI production mission currently assigned to DIA. The MILDEPs would retain a limited authority to retain CI elements organic to warfighting units as is presently the case in the Army and Marine Corps. These latter elements could retain the capability to conduct CI investigations, but under guidelines and central control exerted by DCIA in much the same manner as the services now conduct personnel security investigations on behalf of DIS.

As shown in Figure 2, DCIA's organization focuses on geographic regional commands with subordinate field offices and resident offices to provide CI support down to the installation level. The headquarters for the Europe, Pacific and Americas Regions would be co-located with the theater CINC's headquarters, and the head of each region would have a general support relationship with the CINC's J2. Subordinate field offices would similarly be established in proximity to the headquarters of the theater's component commands, and the resident offices would be positioned to support the major subordinate commands and

installations of each component. The CONUS region would likely be the largest of the major DCIA subordinate elements, and would be charged with supporting not only the CONUS-based CINCs, but also the service major commands composing the sustaining base as well as the various defense agencies and institutes. A fifth major element, equivalent to a region, is the Special Contingency Unit (SCU). In normal peacetime operations, the Washington-based SCU would be relatively lightly manned and would directly support the CJCS, as well as provide CI support within the Pentagon generally. In the event of a contingency operation, the SCU would surge to provide a CI element capable of deploying with the designated contingency forces and providing CI support in the theater of operations for the duration of the contingency.

DIA-Centric Model: ("Directorate for Operations").

As a variant of the OSD-Centric model, the DIA-centric model also removes from the MILDEPs the functions of conducting CI investigations and special operations, but there are several important differences.

In this instance, it is assumed that the Secretary of Defense has decided to concentrate these CI functions at a level above the MILDEPs, but has not gained Congressional authority or not desired to establish a new defense agency for the purpose. Noting DIA's role as the DOD HUMINT manager, the Secretary

DIA-centric Model
Directorate for Operations

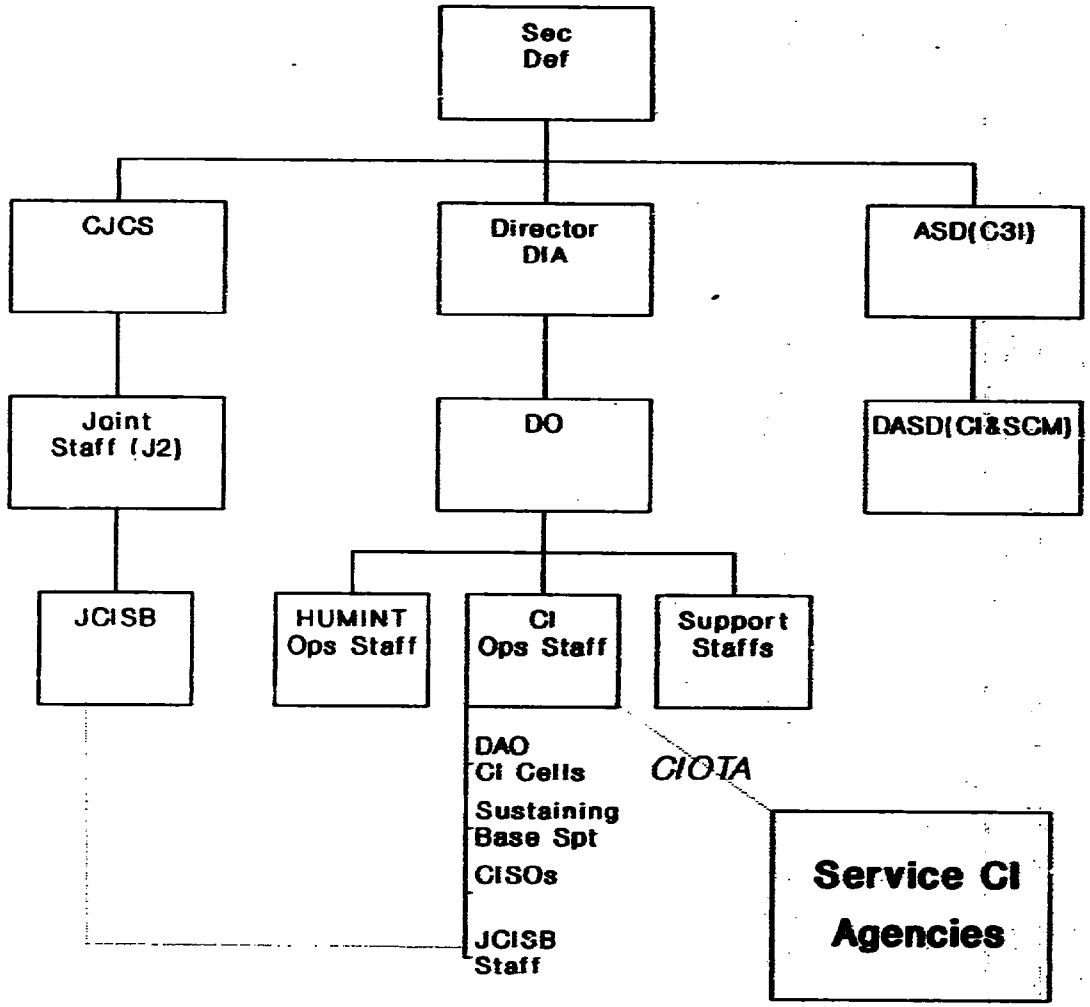

Figure 3. DIA-centric Model

determines to assign the CI functions to DIA, and, with the concurrence of the Director of DIA and Congressional committees, roll them into the existing Directorate of Operations, headed by an Army major general. CI production remains with DIA's Office of Global Analysis, and the role of the existing Office for Security and Counterintelligence is reduced to security management within DIA, and its manpower contribution to the JCISB is realigned to the enlarged Directorate for Operations (DO).

Under an expanded CI charter accorded by ASD(C3I), DIA would structure itself to assume operational management of CI investigations and operations in much the same way as it did for HUMINT operations during 1992. DO would operationally control, manage and coordinate all CI investigations and special operations within DOD, and would be the single point of contact for operational coordination with CIA and FBI.

DO would formally establish for itself CI Operational Tasking Authority (CIOTA) over its own subordinates and the service CI agencies. The premise of CIOTA is derived from the long-standing signals intelligence (SIGINT) Operational Tasking Authority (SOTA) vested in the Director of the National Security Agency (NSA). Under SOTA, NSA directs the operational activities of the strategic collection assets of the service cryptologic agencies without intervention from respective service chains of command. DIA, in enlarging its authority as the DOD HUMINT manager, created a similar HUMINT Tasking Authority (HOTA). Neither SOTA nor HOTA concern themselves directly with tactical

level activities in the respective disciplines, but CIOTA would do so, to the extent that it reaches down to all CI elements in the components of the U&S commands. The CI force structure within the MILDEPs would remain substantially intact, but would receive operational direction and control from DO rather than from service CI agencies or MILDEP headquarters. This configuration also implies that the statutory responsibilities of the MILDEP secretaries remain unchanged.

Under this scheme, DIA also receives some additional manpower spaces to carry out certain CI functions which are deemed more appropriate for direct DIA involvement as opposed to that of the MILDEPs. These direct DIA functions would include overall management of the JCISB, the introduction of CI cells into at least selected DIA Defense Attache Offices (DAOs), the provision of CISOs to the U&S commands and CI support to defense agencies (currently assigned to the MILDEPs as executive agency responsibilities). Placing CI cells in DAOs is calculated to overcome the existing problem of forward basing CI assets in parts of the world where the U.S. military does not have a forward force presence but does have significant potential for involvement in major regional contingencies. Upon assuming the CISO function in the U&S commands, DIA would expand the role of those supporting regional CINCs to include in-theater operational control and coordination of CI investigations and operations carried out by service CI elements.

The notional organization structure depicted in Figure 3 illustrates the DIA-centric model, and accounts for CI support to the sustaining base, as well as for U&S commands. It also highlights a changed and somewhat diminished role for the DASD(CI&SCM). Under current alignments, the Director DIA reports directly to the Secretary of Defense, and in that sense is on the same line as the CJCS and the ASD(C3I). Further, under DIA's scheme of providing functional managers for the various defense intelligence disciplines, the DO, having accrued the necessary operational authorities, would logically become the DOD CI functional manager, just as he is the DOD HUMINT functional manager. This implies also that the DO is the primary official charged with the preparation and management of DOD's Foreign Counterintelligence Program budget, just as he now prepares and manages the HUMINT portion of the General Defense Intelligence Program. This is a function which has hitherto been solely the purview of the DASD(CI&SCM), who would now be reduced to a more general programmatic oversight role. The function of keeping the Secretary of Defense informed of significant CI matters would logically also shift to DIA. DASD(CI&SCM) would, however, retain present policy responsibilities and programmatic oversight.

Joint-Staff-Centric Model: ("J2CI Staffs")

The last of the four models for defense CI to be presented in this paper focuses on the critically important task of

Joint-Staff-Centric Model

J2 CI Staffs

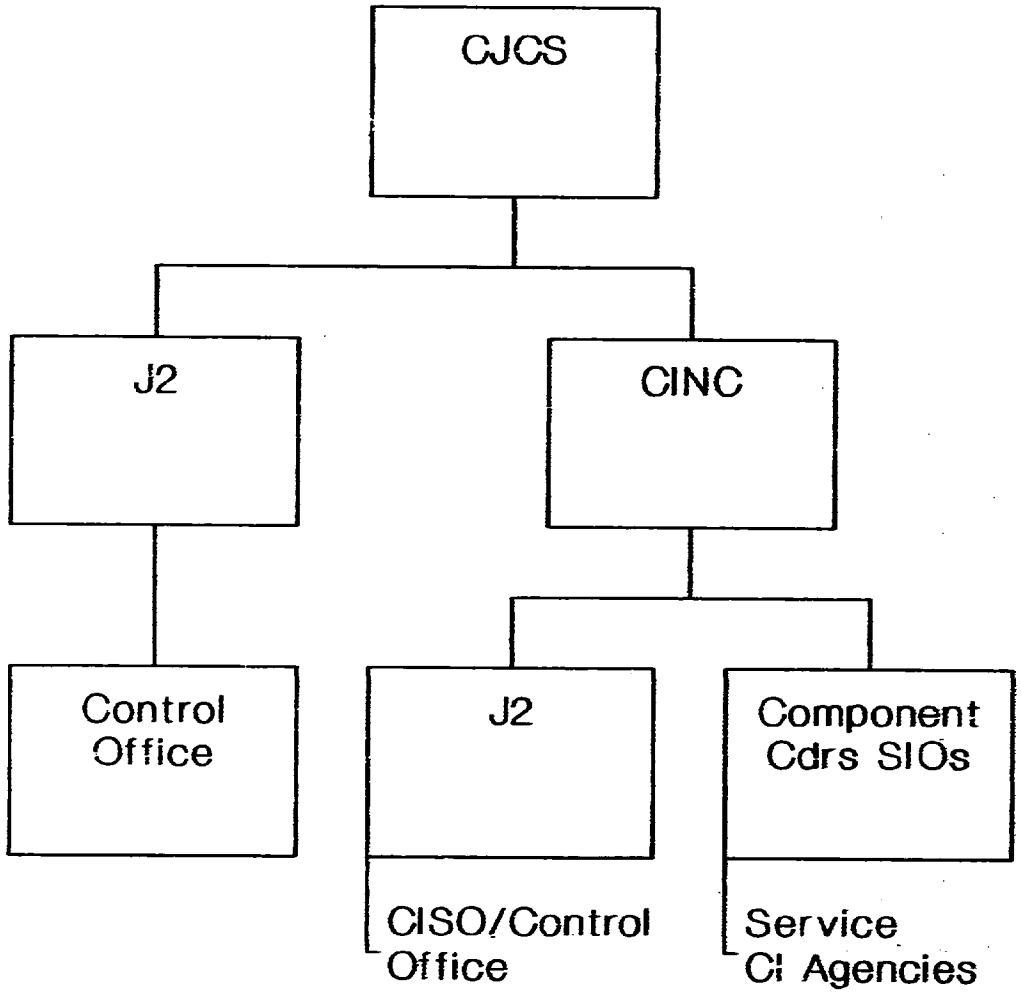

Figure 4. Joint-Staff-Centric Model

providing adequate and responsive CI support to the U&S commands. It assumes that CJCS, as spokesman for the CINCs, has approached the Secretary of Defense with a request that the CINCs be given full operational control over service CI elements supporting forces under the CINCs' combatant command authority. This would strengthen the authorities already outlined in DODI 5240.10. The Secretary approves, invoking Title 10, Section 165.[34] The MILDEP secretaries otherwise retain the administrative chain of command over the service CI elements. It leaves the service CI agencies and force structures intact, but enhances the CINC's operational control of CI activities in the various theaters. It does not concern itself with CI support to defense agencies or service-level sustaining base commands, leaving those functions under the DASD(CI&SCM) and the direction of the service secretaries. It is thus not a complete model for restructuring defense CI, but rather is limited to infusing the Joint Staff with broad authority for planning and strategic direction of CI activities in the combatant commands and the U&S commands with important new authorities embodied in the concept of CIOTA, as described under the DIA-centric model.

CIOTA in the sense of broad strategic operational guidance and staff supervision would be vested in the J2 of the Joint Staff, and the function would be one integral to the Joint Staff, despite DIA's role in manning the J2 staff. The CINCs would exercise CIOTA through the CI Staff Officer (CISO), who becomes an integral part of the CINC's J2 staff rather than a service

detailee as is now generally the case. From the theater level, CIOTA conveys through the senior intelligence officers of the component commands to the service CI elements operating in the theater.

While CIOTA would focus on the direction and technical control of CI investigations and operations, it would also include tasking authority for CI production to DIA and the theater Joint Intelligence Centers as well. CIOTA would also include tasking authority and management of CI collection activities.

The Joint Staff J2's functions and authorities would concurrently be expanded to include the establishment of theater CI priorities as part of his input to JSPS.

As shown in Figure 4, the organizational mechanism for exercising CIOTA is a system of control offices somewhat similar to the present Army system, which in this model would be limited to CI activities in support of CONUS-based forces and the sustaining base.

CHANGE AND THE DESIRED END STATE

How much jointness is enough? A necessary preface to any consideration of changing the organizational structure of Defense CI, particularly where the aim is to enhance unity of effort, is some conclusion as to the desired end state. What should CI look like, functionally? What should be the effects, the value added,

of jointness? Do we need to change the structural paradigm of Defense CI to get there? One way to begin is to establish some clear objectives or principles by which to measure the adequacy of jointness. The foregoing analysis provides the basis for three such principles as a tentative definition of a desired end state for Defense CI.

Principle 1: Ensure responsive support to the combatant commands and their components which reflects unity of effort.

Principle 2: Meet the future strategic challenges for CI in a coherent manner.

Principle 3: Provide for essential interoperability among the service CI agencies, DIA, and the various joint and service staffs. Chiefly, this implies the need for a joint information systems architecture to support Defense CI.

Having established at least the framework for a desired end state, how do we measure a perceived need to change the existing structures against those principles? It may well be that the status quo is adequate, or that relatively minor adjustments in doctrine, interoperability, and the like will achieve the desired result. Two principles, at least, should apply.

Principle 1: Carefully evaluate the long term effects of efficiency and economy that may result from a reorganization against the likely short term costs, institutional perturbation, and personnel disruptions.

Congress and DOD officials who might seek a broader reorganization of Defense CI should keep in mind that the

adoption of any of the three alternative models offered here, or of any variant thereof, will at a minimum produce some less than desirable second and third order effects. To use a popular figure of speech, this will be an emotional "rice bowl" issue for the services. How much institutional crockery can we break before we get a negative return on investment? This is an issue that tends to get short shrift from influential officials determined to effect change. It has enough destructive potential, however, that it deserves consideration as a matter of prudence.

General Colin Powell, in reporting to Congress in early 1993 on the roles, missions, and functions of the Armed Forces, effectively rejected proposals to centralize certain functions. These included theater air defense, chaplains, and the legal corps. In doing so, the CJCS cited factors such as near term costs, personnel disruption, loss of support tailored to service-unique considerations, and insignificant cost savings.[35] He stated:

> We cannot preserve our military strength if we place perceived economy ahead of proper effectiveness, or if we place one Service or component ahead of others. If we proceed too quickly, or impose changes so large they cannot be absorbed, the risk is that we may destroy the basic fabric of our fighting force.[36]

In a much smaller sense, the same applies to Defense CI.

Principle 2: Explicitly develop and articulate the desired end state of organizational change in Defense CI. What should the Defense CI structure look like when we are through tinkering

with it? What must be preserved? What will be better in terms of value added?

Enhanced interoperability should be a primary consideration. Integral to enhanced interoperability is preserving the effectiveness and integrity of the major CI functions (investigations, operations, collection and production).

CI should also maintain its customer service orientation. Many senior CI officials in DOD agree that for CI to provide optimal support, CI agents in the field need extensive knowledge of the commands they serve, and of the services of the commands. A CI agent, however competent, whose background is primarily with the Navy will be hard pressed to deal effectively and credibly with Army or Air Force commanders. One is reminded of the line Meredith Willson's musical comedy *The Music Man*: "You gotta know the territory."

Finally, CI must emerge from any change with responsibility for CI activities and their oversight clearly fixed on identifiable officials. Agents of change will need to have their legal counsel and legislative liaison officers in tow. Any major organizational change involving a shift of CI authorities will almost certainly impact upon the Title 10 responsibilities of the service secretaries. It may well be that legislative action will be a necessary precondition to a major reorganization of Defense CI.

Advantages and disadvantages of the four models.

The MILDEP-centric model, the status quo, is functional, albeit complex and perhaps baffling to someone outside the Defense CI community. Mechanisms such as the Defense CI Board and the new Joint CI Support Branch, as well as the interagency advisory group mentioned earlier have evolved as fora for the discussion and resolution of joint issues and for the promotion of unity of effort. One result has been to build a family of joint CI training courses. These have been useful in terms of building professional skills to a common standard, and show promise of fostering greater commonality of CI doctrine and practice among the services.[37] The CI agencies of the Air Force and Navy have moved toward much closer operational relationships with the major and component commands of their services, in much the same way as the Army has traditionally.[38]

Doctrinal disparity remains, however, but over the years, the service CI agencies have learned to deal with this, and there is agreement on the functional structure of CI at least. On the other hand, the different orientations on law enforcement or intelligence as the foundation for CI have contributed to CI's identity crisis.

There is one other major point of vulnerability in the status quo. Above the level of the MILDEPs, there is no one in charge of CI in the sense of an executive with day-to-day directive operational authority. The SIGINT and HUMINT disciplines have such a manager. That is not to say that CI

needs one, but the lack of one presents an obvious target for those bent on change.

The OSD-centric model, which creates the DCIA, represents a drastic change, but one which undeniably and unambiguously produces jointness and unity of effort. It may well be, however, one of those "changes so large they cannot be absorbed" that General Powell described.[39] Is there perhaps also a "You gotta know the territory" problem? Many in Defense CI think so, and point to the Defense Investigative Service (DIS). They view the history of DIS as a good reason not to create a "purple suit" CI agency for DOD at the expense of the MILDEPs.[40]

When DIS came into being over two decades ago, the MILDEP CI agencies were relieved of the responsibility for conducting personnel security investigations in the U.S.. Initially, newly established DIS offices were manned largely by military CI agents from nearby offices. Over time, DIS phased out the military agents and became a civilianized agency. Nowadays, DIS agents typically have no military background whatever.

This is not to criticize DIS, but simply to point out that such agencies tend to civilianize over time and lose any connection with the MILDEPs to the point where operational personnel do not understand well the entities they are assigned to serve.

Of the three alternative models, the DIA-centric one appears as though it could deal effectively with the "Who's in charge?" issue and at the same time produce relatively little turbulence

in MILDEP force structure. DIA also has well developed institutional ties to both the Joint Staff and the U&S commands. The question here is one of preserving the integrity of CI functions.

How much of CI would DIA want to buy into? Certainly, CI special operations make a reasonably close methodological fit with DIA's HUMINT function. Presently the service CI agencies coordinate these directly with the FBI or CIA as appropriate, and there is no intervening coordination or approval authority at the DOD level. Whether one is needed or not is an arguable issue.

Absorbing the investigative function would create a fairly steep institutional learning curve for DIA, but one which time, experience and the integration of experienced personnel could overcome. DIA already has a dominant role in CI production. It is the assumption of the broad operational area of security advice and assistance to commanders and technical CI services which may be less than appealing to DIA. That is an important operational function, and one that is integral to the customer orientation focus.

Finally, the Joint-Staff-centric model offers assured jointness in the realm of military operations. It also would provide the basis for developing well elaborated joint doctrine, tactics, techniques and procedures. It is, however, an imperfect model as pointed out earlier, in that it does not and could not reasonably deal with the continuing requirements for CI support in the sustaining base. This circumstance places the service CI

agencies in the unenviable position of having to resolve competing requirements for limited CI resources. Unless there would be a clear set of priorities which the Secretary of Defense would establish in this regard, this model could prove to be less than viable. At best, it appears to foster a rupture in the integrity of CI functionality.

CONCLUSION

Defense CI has changed considerably in the past two decades, and especially since the end of the Cold War. Among the various intelligence disciplines, however, CI is peculiar in ways that make the evaluation of the changes difficult.

Early in this paper, we saw the difficulty CI has in making its successes in counterespionage appear to be other than the evidence of failure in security. We discussed at some length CI's identity crisis and the problems with trying to align CI functions with security countermeasures or other intelligence disciplines. More often than not, it is easier for those outside CI to evaluate by its failures than its successes. CI failures, like other types of intelligence failures, tend to be obvious and embarrassingly well publicized, as was the case in the revelations that led to the Dark Age of CI in the 1970s.

On the other hand, CI efforts which are ineffective or absent are often transparent, at least until a war starts. That is when our combatant commanders may learn to their dismay that inadequate CI and security have enabled the enemy to acquire

detailed knowledge of our war plans or has successfully penetrated a classified weapon system program early enough in the procurement cycle to have developed an effective countermeasure.

That Defense CI must move along some path toward jointness is essential to meet the challenges ahead. The path to the joint end state ultimately selected must be well thought out. The foundation is in place in terms of policy and emerging doctrine, but the desired end state is not yet well defined. It is not too soon to start its development. Evaluating jointness in CI by the soundness of whatever evolutionary path may be chosen will likely be easier and hence a better yardstick than rating it by the relative successes and failures of CI operational measures. The framework of principles of change set forth in this paper may prove useful to that end.

Some change in Defense CI structures may be inevitable. These changes need not necessarily be drastic or unpalatable, but they could be, particularly if driven by change agents external to the Defense CI community. Any of the four organizational models offered here can be made to work. That includes the *status quo*, MILDEP-centric model. General Stewart commented: "The present system of component CI organizations is not broken; in fact it is working quite well. . . .[but] the future dictates a more joint CI structure."[41] A better outcome in terms of the overall health of Defense CI will very likely result if as a community it charts its own path to jointness and sets its own agenda for change.

ENDNOTES

1. John F. Stewart, Jr., correspondence with the author, 26 February 1993.

2. Sharon LaFraniere, "House Votes Execution for Spies," Washington Post, 28 June 1985, A1.

3. Harvey L. Holmes, Jr. (ed.), The New York Times Index, 1984: A Book of Record (New York: The New York Times Company, 1985), 449. Idem, The New York Times Index for 1985 (1986), 438; and for 1986 (1987), 465.

4. David B. Ottaway and Walter Pincus, "Counterspy Effort Called Inadequate," Washington Post, 8 October 1986, A1.

5. U. S. President, Executive Order 11905, "United States Foreign Intelligence Activities," 18 February 1976. Idem, Executive Order 12036, "United States Intelligence Activities," 26 January 1978.

6. Department of Defense, Regulation 5240.1R, "Procedures Governing the Activities of DOD Intelligence Components That Affect U. S. Persons," 30 November 1979.

7. Robert W. Singleton, Intelligence Oversight Officer, Office of the Deputy Chief of Staff for Intelligence, Department of the Army, interview by author, Notes, Arlington, Virginia, 3 March 1993. The author is indebted to Mr. Singleton for this account of the history of CI in the 1970s. Mr. Singleton also pointed out that within the Army and DOD generally, restrictions on CI activities were in place long before the publication of DOD Regulation 5240.1R. The earliest relevant policy document he was aware of was a letter by The Adjutant General of the Army dated 1 June 1971 and captioned, "Acquisition of Information Concerning Persons Not Affiliated With the Department of Defense." This letter was known in Army intelligence circles as the "One June Letter."

8. U. S. President, Executive Order 12333, "United States Intelligence Activities," 4 December 1981.

9. Chris Spolar, "Walker Case Has a Long Reach," Washington Post, 30 June 1985, A1.

10. David Hoffman, "President Says Spying On the Rise," Washington Post, 1 December 1985, A1.

11. David B. Ottaway and Walter Pincus, A1.

12. U. S. President, National Security Directive 47, "Counterintelligence and Security Countermeasures," 5 October 1990.

13. David L. Boren, "Rethinking US Intelligence," Defense Intelligence Journal, 1 (Spring 1992): 17-29.

14. U. S. President, National Security Directive 67, "Intelligence Capabilities 1992-2005," 30 March 1992.

15. Department of Defense, DOD Security Review Commission, Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DOD Security Practices and Policies, Washington, D. C., 19 November 1985.

16. Claudia A. Smith, interview by author, Notes, Arlington, Virginia, 25 February 1993.

17. Leif Rosenberger, "Honduras: From Oasis of Peace to Hotbed of Terrorism," unpublished manuscript, Strategic Studies Institute, U. S. Army War College, Carlisle, Pennsylvania, 11 April 1989.

18. U. S. Southern Command, Joint Task Force Bravo, JTF-Bravo 1990 in Perspective (Honduras, Joint Task Force Bravo, June 1990), Preface (unnumbered).

19. Department of Defense, Instruction Number 5240.10, "DOD Counterintelligence Support to Unified and Specified Commands," 18 May 1990.

20. In the Summer of 1991, the author attended the annual DOD Foreign Counterintelligence Conference in Virginia Beach, Virginia. The CISOs attended this conference and each reported on his experiences to date. They were uniformly positive about the CISO concept.

21. Duane Andrews, "Restructuring Defense Intelligence," American Intelligence Journal 12 (Autumn 1991): 5-7.

22. Department of Defense, Office of the Assistant Secretary for Command, Control, Communications and Intelligence, "Counterintelligence Strategic Plan for the 90s," 1 December 1992.

23. Department of Defense, Office of the Chairman, The Joint Chiefs of Staff, MCM-149-92, "Counterintelligence Support," 26 October 1992.

24. Stewart, correspondence with the author.

25. Department of Defense, Chairman of the Joint Chiefs of Staff Report on the Roles, Missions, and Functions of the Armed Forces of the United States, February 1993, xviii, III-32-34.

26. Department of Defense, Joint Publication 2-03 (initial draft), Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Joint Operations, December 1992.

27. Department of Defense, Joint Publication 2-0 (test publication), Doctrine for Intelligence Support to Joint Operations, 30 June 1991.

28. Nicholas J. Ciccarello, Colonel, U. S. Army, interview by author, Notes, Arlington, Virginia, 12 February 1993.

29. Ray W. Pollari, Director of Counterintelligence and Acting Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures), interview by author, Notes, Arlington, Virginia, 12 February 1993.

30. United States Code, Title 10 -- Armed Forces, Section 3013 (1988 edition). This section charges the Secretary of the Army with, among other things, ". . . the effective supervision and control of the intelligence activities of the Department of the Army." Similar responsibilities are assigned to the Secretaries of the Navy and Air Force under sections 5014 and 8014, respectively. See also, e.g., "Legislative History, P. L. 99-433, Goldwater-Nichols Department of Defense Reorganization Act of 1986," in United States Code Congressional and Administrative News, Congress -- Second Session 1986, (St. Paul, Minnesota, West Publishing Co., year not given) 4, 2223: "There has been some confusion over the role of the Secretaries of the Military Departments concerning intelligence activities because of those activities' close association with operational matters. Clause (7) would end this confusion by specifying that the Secretary of the Army is responsible for the Army's intelligence activities."

31. United States Code, Title 10, Section 165. Title 10 is less explicit about the responsibilities of the Secretary of Defense for intelligence matters than for the service secretaries. Section 165 does provide, however, that the Secretary of Defense has the discretionary authority to assign responsibilities of the military department secretaries for administration and support to combatant commands or Defense agencies.

32. Kenneth Krantz, Chief, Joint Counterintelligence Support Branch, interview by author, Notes, Arlington, Virginia, 20 November 1992.

33. Ibid.

34. See note 31 above.

35. Report on Roles, Missions, and Functions, February 1993, xviii-xx.

36. Ibid., I-12.

37. Pollari, interview by author.

38. Robert A. Hoffman, Brigadier General (Select), U. S. Air Force, Director of Criminal Investigations and Counterintelligence, Office of the Air Force Inspector General, interview by author, Notes, Arlington, Virginia, 12 February 1993. Pollari, interview by author.

39. Report on Roles, Missions, and Functions, I-12.

40. Pollari, interview by author. Stewart, correspondence with author. Both Mr. Pollari and General Stewart felt that neither rolling CI into DIS nor creating a DIS-like agency as the primary Defense CI resource would be successful in improving Defense CI, and likely would be detrimental. General Stewart opined that a future joint CI organization must include both military and civilian personnel, and that military members assigned need to be ". . . fully qualified soldiers who understand their service and how it works prior to becoming part of a joint organization."

41. Stewart, correspondence with the author.

BIBLIOGRAPHY

Andrews, Duane. "Restructuring Defense Intelligence." American Intelligence Journal 12 (Autumn 1991): 5-7.

Boren, David L.. "Rethinking US Intelligence." Defense Intelligence Journal 1 (Spring 1992): 17-29.

Ciccarello, Nicholas J., Colonel, U. S. Army. Interview by author, 12 February 1993. Arlington, Virginia. Notes.

Department of Defense. Chairman of the Joint Chiefs of Staff Report on the Roles, Missions, and Functions of the Armed Forces of the United States. February 1993.

_____, DOD Security Review Commission. Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DOD Security Practices and Policies. Washington, D. C., 19 November 1985.

_____. Instruction Number 5240.10. "DOD Counterintelligence Support to Unified and Specified Commands." 18 May 1990.

_____. Joint Publication 2-0 (test publication). Doctrine for Intelligence Support to Joint Operations. 30 June 1991.

_____. Joint Publication 2-03 (initial draft). Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Joint Operations. December 1992.

_____, Office of the Assistant Secretary for Command, Control, Communications and Intelligence. "Counterintelligence Strategic Plan for the 90s." 1 December 1992.

_____, Office of the Chairman, The Joint Chiefs of Staff. MCM-149-92. "Counterintelligence Support." 26 October 1992.

_____. Regulation 5240.1R. "Procedures Governing the Activities of DOD Intelligence Components That Affect U. S. Persons." 30 November 1979.

Hoffman, David. "President Says Spying On the Rise." Washington Post. 1 December 1985, A1.

Hoffman, Robert A., Brigadier General (Select), U. S. Air Force, Director of Criminal Investigations and Counterintelligence, Office of the Air Force Inspector General. Interview by author, 12 February 1993. Arlington, Virginia. Notes.

Holmes, Harvey L. (ed.). The New York Times Index 1984: A Book of Record. New York: The New York Times Company, 1985.

_____. The New York Times Index 1985: A Book of Record, New York: The New York Times Company, 1986.

_____. The New York Times Index 1986: A Book of Record, New York: The New York Times Company, 1987.

Krantz, Kenneth, Chief, Joint Counterintelligence Support Branch, Defense Intelligence Agency. Interview by author, 20 November 1992. Arlington, Virginia. Notes.

LaFraniere, Sharon, "House Votes Execution for Spies." Washington Post. 28 June 1985, A1.

Ottaway, David B. and Pincus, Walter. "Counterspy Effort Called Inadequate." Washington Post. 8 October 1986, A1.

Pollari, Ray W., Director of Counterintelligence and Acting Deputy Assistant Secretary of Defense (Counterintelligence and Security Countermeasures). Interview by author, 12 February 1993. Arlington, Virginia. Notes.

Rosenberger, Leif. "Honduras: From Oasis of Peace to Hotbed of Terrorism." Unpublished manuscript. Files, Strategic Studies Institute, U. S. Army War College, Carlisle, Pennsylvania. 11 April 1989.

Singleton, Robert W., Intelligence Oversight Officer, Office of the Deputy Chief of Staff for Intelligence, Department of the Army. Interview by author, 3 March 1993. Arlington, Virginia. Notes.

Smith, Claudia A.. Interview by author, 25 February 1993. Arlington, Virginia. Notes.

Spolar, Chris. "Walker Case Has a Long Reach." Washington Post. 30 June 1985, A1.

Stewart, John F., Jr., Major General, U. S. Army. Correspondence with the author, 26 February 1993.

United States Code. Title 10 -- Armed Forces (1988 edition).

U. S. President. Executive Order 11905. "United States Foreign Intelligence Activities." 18 February 1976.

_____. Executive Order 12036. "United States Intelligence Activities." 26 January 1978.

_____. Executive Order 12333. "United States Intelligence Activities." 4 December 1991.

_____. National Security Directive 47. "Counterintelligence and Security Countermeasures." 5 October 1990.

_____. National Security Directive 67. "Intelligence Capabilities 1992-2005." 30 March 1992.

U. S. Southern Command, Joint Task Force Bravo. JTF-Bravo 1990 in Perspective. Honduras: Joint Task Force Bravo, June 1990.